

ON THE MAXIMAL WEIGHT OF (P, Q) -ARY CHAIN PARTITIONS WITH BOUNDED PARTS

FILIPPO DISANTO, LAURENT IMBERT, AND FABRICE PHILIPPE

ABSTRACT. A (p, q) -ary chain is a special type of chain partition of integers with parts of the form $p^a q^b$ for some fixed integers p and q . In this note, we are interested in the maximal weight of such partitions when their parts are distinct and cannot exceed a given bound m . Characterizing the cases where the greedy choice fails, we prove that this maximal weight is, as a function of m , asymptotically independent of $\max(p, q)$, and we show how to compute its value in logarithmic time.

1. INTRODUCTION

Let p, q be two fixed integers, and let $E = \{p^a q^b : (a, b) \in \mathbb{N}^2\}$ be endowed with the divisibility order, i.e. $x \succeq y \iff y \mid x$. A (p, q) -ary chain is a finite non-increasing sequence in E . For example, $(72, 12, 4, 4, 1)$ is a $(2, 3)$ -ary chain, whereas $(72, 12, 4, 3, 1)$ is not since $4 \not\succeq 3$. We define the *weight* of a (p, q) -ary chain as the sum of its terms, i.e. an expression of the form

$$w = \sum_{i \geq 1} p^{a_i} q^{b_i}, \quad \text{where } p^{a_i} q^{b_i} \succeq p^{a_{i+1}} q^{b_{i+1}} \text{ for } i \geq 1. \quad (1)$$

Expansions of this type have been proposed and successfully used by Dimitrov in the context of digital signal processing or cryptography under the name *double-base number system*. For more details, see [1, 2] and the references therein.

From a different point of view, a (p, q) -ary chain can be seen as a partition of its weight, where the parts are restricted to the set E and constrained by a divisibility condition. Surprisingly, works on integer partitions with divisibility constraints on the parts are very scarce. Erdős and Loxton [3] considered two types of such unconventional partitions, called chain and umbrella partitions, and obtained “some rather weak estimates for various partition functions”. More recently, motivated by some theoretical questions behind Dimitrov’s number system, the second and third authors refined some of Erdős and Loxton’s earlier results in a paper [4] dedicated to *strictly chained (p, q) -ary partitions*. A strictly chained (p, q) -ary partition, or (p, q) -SCP for short, is a decreasing (p, q) -ary chain, i.e. it has distinct parts. In this note, we are interested in the maximal weight of a (p, q) -SCP whose parts are bounded by some given integer m . In particular, assuming $p < q$, we prove that this maximal weight asymptotically grows as $pm/(p-1)$, independently of q .

The heaviest (p, q) -SCP whose first part is *given* may be computed using a greedy strategy: successively take the next greatest part satisfying the divisibility condition. Nevertheless, given a bound $m > 0$ on the parts, determining how to best select the first part is not immediate and the greedy approach appears to fail as a

general rule. That is, choosing the largest part less than or equal to m does not always provide a partition of maximal weight. These facts are established in Sections 2 and 3 among other preliminary definitions, examples, and results. The cases where the greedy choice fails are fully characterized in Section 4, while Section 5 is devoted to the asymptotic behavior of the maximal weight as a function of bound m . Finally, it is explained in Section 6 how to compute a best choice for the first part, thus the maximal weight, in $O(\log \log m)$ time.

It is worthwhile to point out that our results still hold for any pair of multiplicatively independent algebraic numbers p, q .

2. PRELIMINARIES

Let m be a positive integer, and let $G(m)$ denote the maximal weight of a (p, q) -SCP whose greatest part does not exceed m . For example, with $p = 2$ and $q = 3$, the first values of G are: 1, 3, 4, 7, 7, 10, 10, 15, 15, 15, 15, 22, 22, 22, 22, 31, 31, \dots

In the following, we shall assume w.l.o.g. that $p < q$. Notice that the case $p = 1$ is irrelevant since $G(m)$ is simply the sum of all the powers of q less than or equal to m . More generally, and for the same reason, we shall consider that p and q are not powers of the same integer, that is, they are *multiplicatively independent* (see, e.g., [5] Th. 2.5.7). Under this assumption, the first values of $G(m)$ may be quickly computed with the help of the following formula.

Proposition 1. *For $m \in \mathbb{N}^*$, let $G(m)$ denote the largest integer that can be expressed as a strictly chained (p, q) -ary partition with all parts less than or equal to m . Assume that $G(m) = 0$ if $m \notin \mathbb{N}$. Then, we have $G(1) = 1$, and for $m > 1$*

$$G(m) = \max(G(m-1), 1 + pG(m/p), 1 + qG(m/q)). \quad (2)$$

Proof. Let λ be a partition of weight $G(m)$ whose parts are all less than or equal to m . First, notice that λ must contain part 1 by definition of $G(m)$. If m is not an element of E , then $G(m) = G(m-1)$. Otherwise, it suffices to note that removing part 1 in λ produces a partition whose parts are all divisible by either p or q . \square

Computing $G(m)$ with relation (2) requires $O(\log m)$ steps in the worst case: simply note that, for all m , in at most $p-1$ baby-steps, i.e. $G(m) = G(m-1)$, one gets an integer that is divisible by p . Formula (2) may also be adapted to provide a (p, q) -SCP of weight $G(m)$. Nevertheless, it does not give any idea about the asymptotic behavior of G . Moreover, we shall see in Section 6 how to compute $G(m)$ and a (p, q) -SCP of weight $G(m)$ in $O(\log \log m)$ time.

A natural graphic representation for (p, q) -SCPs obtains by mapping each part $p^a q^b \in E$ to the pair $(a, b) \in \mathbb{N}^2$. Indeed, with the above assumptions on p and q , the mapping $(a, b) \mapsto p^a q^b$ is one-to-one. Since the parts of a (p, q) -SCP are pairwise distinct by definition, this graphic representation takes the form of an increasing path in \mathbb{N}^2 endowed with the usual product order. This is illustrated in Figure 1 with the ten $(2, 3)$ -SCPs containing exactly six parts and whose greatest part equals $72 = 2^3 3^2$. Note that a (p, q) -SCP with largest part $p^a q^b$ has at most $a + b + 1$ parts, and there are exactly $\binom{a+b}{b}$ of them with a maximum number of parts.

With this representation in mind, one is easily convinced that the heaviest (p, q) -SCP with first part $p^a q^b$ looks like the top left (p, q) -SCP in Figure 1. This is formalized in the following lemma.

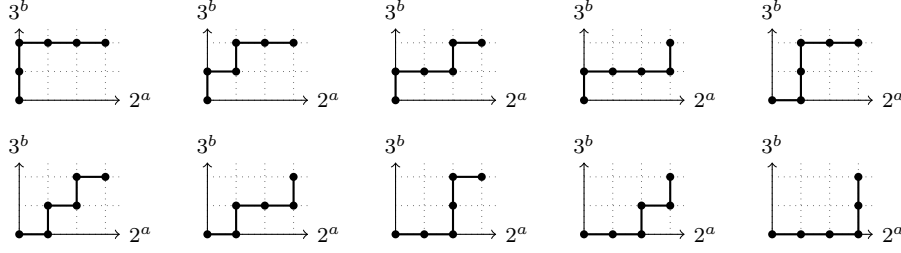


FIGURE 1. The set of $(2, 3)$ -SCPs with 6 parts and whose largest part equals $2^3 3^2 = 72$.

Lemma 1. *Given $a, b \in \mathbb{N}$, the heaviest (p, q) -SCP with first part $p^a q^b$ is the one whose parts are the elements of the set $\{q^i : 0 \leq i < b\} \cup \{q^b p^i : 0 \leq i \leq a\}$.*

Proof. Consider a (p, q) -SCP $\lambda = (\lambda_i)_{i=1}^k$ with greatest part $\lambda_1 = p^a q^b$. Let $\lambda_i = p^{a_i} q^{b_i}$. If $a_i + b_i > b$ then define $\lambda'_i = p^{a_i + b_i - b} q^b$, otherwise let $\lambda'_i = q^{a_i + b_i}$. Note that $\lambda'_1 = p^a q^b$ again. Since sequence $(a_i + b_i)_{i=1}^k$ is decreasing, $(\lambda'_i)_{i=1}^k$ is also a (p, q) -SCP. Since $p < q$ we have $\lambda'_i \geq \lambda_i$ for all i , with equality if, and only if, the parts in λ form a subset of $\{q^i : 0 \leq i < b\} \cup \{p^i q^b : 0 \leq i \leq a\}$. Therefore, the maximal weight is reached when taking the whole set, and only in this case. \square

As a consequence, a (p, q) -SCP of weight $G(m)$ and whose parts do not exceed m is characterized by its greatest part only. Moreover, denoting by $p^a q^b$ this greatest part, we have $G(m) = h(a, b)$, where h is the mapping defined on \mathbb{N}^2 by

$$h(a, b) = \frac{q^b - 1}{q - 1} + \frac{p^{a+1} - 1}{p - 1} q^b. \quad (3)$$

Accordingly, the definition of G may be rewritten as

$$G(m) = \max_{P_m} h, \quad \text{where } P_m = \{(a, b) \in \mathbb{N}^2 : p^a q^b \leq m\}. \quad (4)$$

Finally observe that the greatest part of a (p, q) -SCP of weight $G(m)$ and whose parts do not exceed m must be a maximal element of $E \cap [0, m]$ for the divisibility order. Otherwise, the partition could be augmented by a part, resulting in a partition of larger weight. The next Section is devoted to the set of these maximal elements.

3. ON THE SET Z_m

Let us denote by Z_m the set of all maximal elements in $E \cap [0, m]$ for the divisibility order. For convenience, we further denote by ρ the logarithmic ratio of q and p , i.e.

$$\rho = \frac{\log q}{\log p} > 1.$$

Since p and q are multiplicatively independent, ρ is irrational. Notice that the elements of E may also be written as $E = \{p^{a+b\rho} : (a, b) \in \mathbb{N}^2\}$. There are exactly $\lfloor \log_q m \rfloor + 1$ elements in Z_m , described in the Lemma below.

Lemma 2. *Let m be a positive integer. The following characterization holds:*

$$p^a q^b \in Z_m \iff 0 \leq b \leq \lfloor \log_q m \rfloor \text{ and } a = \lfloor \log_p m - b\rho \rfloor.$$

Proof. An element $p^a q^b$ of E is in Z_m if, and only if, a and b are non-negative, $p^a q^b \leq m < p^{a+1} q^b$, and $p^a q^b \leq m < p^a q^{b+1}$. Since $p < q$, the latter condition is superfluous. It is easy to check that the remaining conditions are equivalent to the Lemma's claim. \square

As an immediate consequence, let us note for further use that

$$Z_{qm} = qZ_m \cup \{p^{\lfloor \rho + \log_p m \rfloor}\}, \quad (5)$$

$$Z_{pm} = \begin{cases} pZ_m & \text{if } \lfloor 1/\rho + \log_q m \rfloor = \lfloor \log_q m \rfloor, \\ pZ_m \cup \{q^{\lfloor \log_q m \rfloor + 1}\} & \text{otherwise.} \end{cases} \quad (6)$$

The elements of Z_m correspond exactly to the maximal integer points below or on the line of equation $a \log p + b \log q - \log m = 0$. An example is given in Figure 2. The corresponding values $p^a q^b$ and $h(a, b)$ are reported in Table 1.

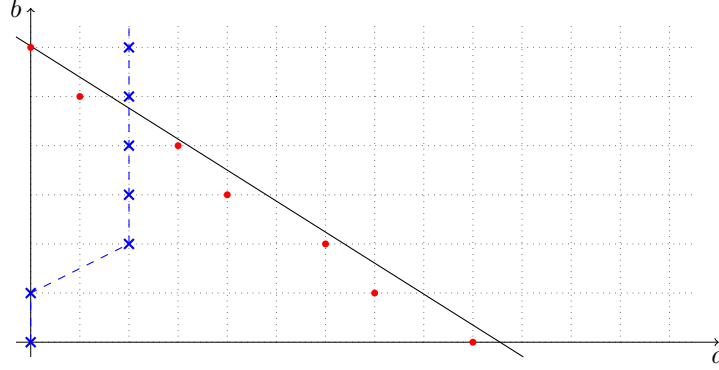


FIGURE 2. The set Z_{750} for $(p, q) = (2, 3)$, represented as all maximal integer points below the line of equation $x \log 2 + y \log 3 - \log 750 = 0$. The points along the dashed line correspond to the first values of the sequence ℓ defined in Theorem 1.

| (a, b) | $(0, 6)$ | $(1, 5)$ | $(3, 4)$ | $(4, 3)$ | $(6, 2)$ | $(7, 1)$ | $(9, 0)$ |
|-----------|----------|----------|----------|----------|----------|----------|----------|
| $p^a q^b$ | 729 | 486 | 648 | 432 | 576 | 384 | 512 |
| $h(a, b)$ | 1093 | 850 | 1255 | 850 | 1147 | 766 | 1023 |

TABLE 1. The elements of Z_{750} for $(p, q) = (2, 3)$, together with the corresponding values $p^a q^b$ and $h(a, b)$. Note that $G(750) = h(3, 4) = 1255$.

Further define z_m as the greatest integer of the form $p^a q^b$ less than or equal to m , that is,

$$z_m = \max Z_m.$$

Since $q^{\lfloor \log_q m \rfloor} \in Z_m$, we have $z_m \rightarrow \infty$ when $m \rightarrow \infty$. The next Proposition goes one step further.

Proposition 2. *We have the following: $z_m \sim m$ when $m \rightarrow \infty$.*

Proof. Let \hat{z}_m be the smallest integer of the form $p^a q^b$ greater than or equal to m . Thus we have $z_m \leq m \leq \hat{z}_m$. By a theorem of Tijdeman [6] we know that, for m large enough, there exists a constant $C > 0$ such that

$$\hat{z}_m - z_m < \frac{z_m}{(\log z_m)^C},$$

so that $0 \leq m - z_m < z_m / (\log z_m)^C$. \square

From a greedy point of view, one might think that taking z_m as the largest part of the (p, q) -SCP formed as in Lemma 1 yields a (p, q) -SCP of weight $G(m)$; in which case our asymptotics problem would be solved using the above Proposition. Unfortunately, this is not true. In Table 1, we see for instance that $z_{750} = 729$, obtained for $(a, b) = (0, 6)$, does not give a (p, q) -SCP of maximal weight. Instead, the maximal weight $G(750)$ is $h(3, 4) = 1255$. Hence, even if m is of the form $p^a q^b$, the first part of a (p, q) -SCP of maximal weight may be different from m . For instance $G(729) = 1255$ obtains from a unique (p, q) -SCP whose first part is 648. In the next Section, we study the subset Y_m of Z_m yielding the heaviest (p, q) -SCPs, i.e. those of maximal weight $G(m)$.

4. ON THE SET Y_m

According to (4), $G(m)$ is equal to $h(a, b)$ for certain values a, b . First notice that these values are not necessarily unique with respect to this property, because h is not necessarily one to one. As an example, in Table 1, we observe that with $(p, q) = (2, 3)$ we have $h(1, 5) = h(4, 3) = 850$. Similarly, with $(p, q) = (2, 5)$ we have $h(0, 2) = h(4, 0) = 31$.

Let Y_m be the set of all elements $p^a q^b$ in $E \cap [0, m]$ such that $h(a, b) = G(m)$. As already noticed, Y_m is a subset of Z_m . Next recall that $z_m = \max Z_m$ needs not be in Y_m . A particular link between Y_m and z_m however exists, given in the following Proposition.

Proposition 3. *For $m \in \mathbb{N}^*$, let $z_m = p^a q^b$. Then*

$$Y_m \subset \{p^i q^j \in Z_m : j \leq b\}. \quad (7)$$

Proof. Using (3), we have

$$\begin{aligned} \frac{p-1}{p} h(a, b) &= \frac{p-1}{p} \frac{q^b - 1}{q - 1} + \frac{q^b}{p} (p^{a+1} - 1) \\ &= p^a q^b - q^b \frac{q-p}{pq-p} - \frac{p-1}{p(q-1)}, \end{aligned}$$

so that

$$h(a, b) = \frac{p}{p-1} (p^a q^b - r q^b) - \frac{1}{q-1}, \quad \text{where } r = \frac{q-p}{pq-p} \in (0, 1/p). \quad (8)$$

Note that $0 < r < 1/p$, because $pq - p > p(q - p)$. As a consequence, we get

$$h(a, b) > h(a', b') \iff p^a q^b - p^{a'} q^{b'} > r(q^b - q^{b'}). \quad (9)$$

If $p^{a'} q^{b'} \in Z_m$ we have $z_m = p^a q^b > p^{a'} q^{b'}$. Hence $b' > b$ implies $h(a, b) > h(a', b')$, which concludes the proof. \square

Geometrically, the above Proposition tells us that the points $(a, b) \in \mathbb{N}^2$ such that $h(a, b) = G(m)$ cannot be located “above” or equivalently “left” of z_m . In particular, when $z_m = p^a$, we have $G(m) = h(a, 0) = (p^{a+1} - 1)/(p - 1)$.

In Proposition 4, we will see that the set Y_m has at most two elements. For now, let us first focus on those elements of E that provide the heaviest (p, q) -SCP in a unique way, i.e. those for which $Y_{p^a q^b} = \{p^a q^b\}$. The following Theorem shows that the corresponding points in \mathbb{N}^2 form an infinite area whose boundary is a particular sequence, as illustrated in Figure 2.

Theorem 1. *There exists a sequence $\ell = (\ell_b)_{b \in \mathbb{N}}$ in \mathbb{N} such that*

$$Y_{p^a q^b} = \{p^a q^b\} \iff a \geq \ell_b. \quad (10)$$

Moreover, the sequence ℓ is non-decreasing, unbounded, and satisfies $\ell_0 = 0$.

Proof. Let us first establish the following statements:

- (i) For all $b \geq 0$, there exists $a \geq 0$ such that $p^a q^b \in Y_{p^a q^b}$.
- (ii) If $p^a q^b \in Y_{p^a q^b}$ then, for all $k \geq 1$, $Y_{p^{a+k} q^b} = \{p^{a+k} q^b\}$.

Let $b \in \mathbb{N}$. As already seen, the mapping $(i, j) \mapsto p^i q^j$ is one-to-one. Therefore, we have $q^b - p^i q^j \geq 1$ for all $p^i q^j \in Z_{q^b} \setminus \{q^b\}$. Choose a such that

$$p^a \geq r(q^b - 1), \quad \text{where } r = \frac{q - p}{pq - p} \text{ as in (8).}$$

Then, for all $p^i q^j \in Z_{q^b}$ with $j < b$, we have

$$p^a q^b - p^{a+i} q^j \geq p^a \geq r(q^b - 1) \geq r(q^b - q^j). \quad (11)$$

Using (9), it follows that $h(a, b) \geq h(a + i, j)$; in other words $p^a q^b \in p^a Z_{q^b}$. According to Prop. 3, we also have $Y_{p^a q^b} \subset \{p^i q^j \in Z_{p^a q^b} : j \leq b\}$. Using Lemma 2, it is immediate to check that the latter set is identical to $p^a Z_{q^b}$, thus $p^a q^b \in Y_{p^a q^b}$ and (i) is proved. Now, if $p^a q^b \in Y_{p^a q^b}$ then replacing a by $a + k$ for any $k \geq 1$ turns (11) into a strict inequality. Therefore, $Y_{p^{a+k} q^b} = \{p^{a+k} q^b\}$, and (ii) is proved too. Accordingly, letting

$$\ell_b = \min \{a \in \mathbb{N} : Y_{p^a q^b} = \{p^a q^b\}\} \quad (12)$$

provides the claimed sequence ℓ . Since $Y_1 = \{1\}$ and $1 = p^0 q^0$, we get $\ell_0 = 0$.

Let us now prove that ℓ is non-decreasing. Given $b \in \mathbb{N}$, either $\ell_b = 0$ thus $\ell_{b+1} \geq \ell_b$, or $\ell_b \geq 1$. In the latter, there exists $p^i q^j \in Z_{p^{\ell_b-1} q^b}$ such that $j \neq b$ and $h(i, j) \geq h(\ell_b - 1, b)$. From (3), it is not difficult to see that $h(i, j+1) = qh(i, j) + 1$, and thus $h(i, j+1) - h(\ell_b - 1, b+1) = q(h(i, j) - h(\ell_b - 1, b))$. Therefore $h(i, j+1) \geq h(\ell_b - 1, b+1)$, so that $\ell_{b+1} > \ell_b - 1$.

Finally suppose that ℓ is bounded. This would imply that there exists an integer a such that, for all $b \in \mathbb{N}$, $Y_{p^a q^b} = \{p^a q^b\}$. The following statement shows that this is impossible.

- (iii) For all $a \in \mathbb{N}$ there exists $b \in \mathbb{N}$ such that $h(a + \lfloor b\rho \rfloor, 0) > h(a, b)$.

Indeed, by Lemma 2 we know that $p^{a+\lfloor b\rho \rfloor} \in Z_{p^a q^b}$. Fix $a \in \mathbb{N}$, choose $b \in \mathbb{N}^*$, and set $a' = a + \lfloor b\rho \rfloor$, where $\rho = \log q / \log p$. According to (9), and denoting by

$\{b\rho\} = b\rho - \lfloor b\rho \rfloor$ the fractional part of $b\rho$, we have

$$\begin{aligned} h(a, b) < h(a', 0) &\Leftrightarrow p^a q^b - p^{a'} < r(q^b - 1), \\ &\Leftrightarrow p^{\lfloor b\rho \rfloor} > q^b (1 - r/p^a (1 - 1/q^b)), \\ &\Leftrightarrow \{b\rho\} < -\log_p (1 - r/p^a (1 - 1/q^b)). \end{aligned} \quad (13)$$

Now observe that sequence $(\phi_{a,b})_{b \in \mathbb{N}}$ defined by

$$\phi_{a,b} = -\log_p \left(1 - \frac{r}{p^a} \left(1 - \frac{1}{q^b} \right) \right) \quad (14)$$

is increasing, with $\phi_{a,0} = 0$. Since ρ is irrational, we know that $(b\rho)_{b \in \mathbb{N}}$ is equidistributed modulo 1. Thus, there exists $b > 0$ such that $\{b\rho\} < \phi_{a,1}$, hence $\{b\rho\} < \phi_{a,b}$, which using (13) concludes the proof. \square

Let us anticipate a result of the next section, implying that the sequence ℓ is completely known as soon as we can compute its *jump indices*, that is, the values $b > 0$ for which $\ell_b > \ell_{b-1}$. Indeed, we shall establish with statement (25) that if b is a jump index of ℓ then $\ell_b = \lfloor \alpha(b) \rfloor$, where

$$\alpha(b) = \log_p \frac{1 - q^{-b}}{1 - p^{-\{b\rho\}}} + \log_p \frac{q - p}{q - 1}. \quad (15)$$

Computing the jump indices of ℓ may be done recursively as shown in the next Corollary. Referring to the sequence ϕ defined in (4), let the mapping β be defined on \mathbb{N} by

$$\beta(a) = \min \left\{ j \in \mathbb{N} : j > 0, \{j\rho\} < \phi_{a,j} \right\}. \quad (16)$$

Corollary 1. *The increasing sequence $(b_k)_{k \in \mathbb{N}}$ of the jump indices of ℓ satisfies*

$$b_0 = \beta(0), \quad b_{k+1} = \beta(\ell_{b_k}).$$

Proof. Given any $a \in \mathbb{N}$, we know that $Y_{p^a} = \{p^a\}$ by Prop. 3. Moreover, letting b be incremented by 1 from 0 iteratively, it follows from (5) and (9) that $Y_{p^a q^b} = \{p^a q^b\}$ as long as $h(a, b) > h(a + \lfloor b\rho \rfloor, 0)$. As it is shown in part (iii) of the proof of Theorem 1, the latter inequality is equivalent to $\{b\rho\} < \phi_{a,b}$. Accordingly, $Y_{p^a q^b} = \{p^a q^b\}$ if $b < \beta(a)$. Hence $\ell_{\beta(a)-1} \leq a < \ell_{\beta(a)}$, so that $\beta(a)$ is a jump index for ℓ . The result follows immediately since ℓ is non-decreasing. \square

As claimed before, we next show that Y_m has at most 2 elements. This might be established by directly using (9) and studying the diophantine equation

$$p^a q^b - p^c = r(q^b - 1), \quad \text{where } r = \frac{q - p}{pq - p}.$$

Unfortunately, the latter is seemingly not easy to cope with, whereas Theorem 1 proves handy.

Proposition 4. *For all $m \in \mathbb{N}$, the set Y_m has either one or two elements.*

Proof. Assume $\#Y_m \geq 2$ and denote by $p^a q^b$ its greatest element. Since $Y_m = Y_{p^a q^b}$, we have $a < \ell_b$ by definition of sequence ℓ in Theorem 1. To be more precise, statement (ii) in the proof of this theorem even tells us that $a = \ell_b - 1$. Now let $p^c q^d$ be the second greatest element in Y_m . According to Prop. 3 we must have $d < b$, thus $c > a$ by Lemma 2. Since ℓ is non-decreasing, it follows that $\ell_d \leq \ell_b$. Since $a = \ell_b - 1$ we get $c \geq \ell_d$, which means that $Y_{p^c q^d} = \{p^c q^d\}$ from Theorem 1.

Therefore, there cannot be a third element in Y_m as it would also be an element of $Y_{p^c q^d}$. \square

5. ASYMPTOTIC BEHAVIOR OF G

Our goal in this Section is to prove that $G(m)$ is equivalent to $mp/(p-1)$ as m tends to infinity, independently of q . As a simple first step, let us exhibit a sharp upper bound for G .

Lemma 3. *For all $m \in \mathbb{N}$ and all $n \in Y_m$, we have $G(m) < np/(p-1)$. In particular,*

$$\limsup_{m \rightarrow \infty} \frac{G(m)}{m} = \frac{p}{p-1}.$$

Proof. Let $n = p^a q^b \in Y_m$. According to (8) we have

$$h(a, b) - \frac{np}{p-1} = - \left(\frac{rpq^b}{p-1} + \frac{1}{q-1} \right) < 0, \quad \text{where } r \in (0, 1/p). \quad (17)$$

Hence $G(m) = h(a, b) < np/(p-1)$. Since $n \leq m$, it follows that $G(m)/m \leq p/(p-1)$. To conclude, observe that for $m = p^a$ we have $G(p^a) = (p^{a+1} - 1)/(p-1)$ from Prop 3. Therefore, $\lim_{a \rightarrow \infty} G(p^a)/p^a = p/(p-1)$. \square

Let us now define a mapping y as follows: For all m , let y_m denote the smallest integer of the form $p^a q^b$ such that $G(m) = h(a, b)$, that is

$$y_m = \min Y_m. \quad (18)$$

According to Proposition 3, y_m is also the element of Y_m with the smallest exponent in q . We shall next give a characterization of y_m using the sequence ℓ defined in Theorem 1. Recall that this sequence is defined by $\ell_b = \min\{a \in \mathbb{N} : Y_{p^a q^b} = \{p^a q^b\}\}$ and satisfies (10). Since ℓ is non-decreasing, the sequence $(p^{\ell_b} q^b)_{b \in \mathbb{N}}$ is increasing. We may thus define, for all $m \in \mathbb{N}$,

$$m_\ell = \max\{b \in \mathbb{N} : p^{\ell_b} q^b \leq m\}. \quad (19)$$

Theorem 2. *For all $m \in \mathbb{N}$, we have*

$$y_m = \max\{p^a q^b \in Z_m : b \leq m_\ell\}. \quad (20)$$

Moreover, let $\bar{a} = \lfloor \log_p m - m_\ell \rho \rfloor$ and $\bar{m} = \lfloor m/p^{\bar{a}} \rfloor$. Then $y_m = p^{\bar{a}} z_{\bar{m}}$.

Proof. Let $y_m = p^i q^j$. Since $y_m = \min Y_m$, we have $Y_{y_m} = \{y_m\}$ thus $i \geq \ell_j$ using (10). Suppose $j > m_\ell$, then $p^i q^j \geq p^{\ell_j} q^j$, and thus $p^i q^j > m$ from (19), which contradicts the fact that $y_m \leq m$. Therefore, $j \leq m_\ell$.

Now consider any $p^a q^b \in Z_m$ such that $b \leq m_\ell$. Since ℓ is non-decreasing we have $\ell_{m_\ell} \geq \ell_b$. By Lemma 2, there exists $k \in \mathbb{N}$ such that $p^k q^{m_\ell} \in Z_m$, and we have $k \geq \ell_{m_\ell}$ because $p^{\ell_{m_\ell}} q^{m_\ell} \leq m$. Since $p^a q^b \in Z_m$, condition $b \leq m_\ell$ implies that $a \geq k$ by Lemma 2 again, so that $a \geq \ell_{m_\ell} \geq \ell_b$. Therefore, $Y_{p^a q^b} = \{p^a q^b\}$. Supposing $p^a q^b > p^i q^j$ would then imply that $h(i, j) < h(a, b)$, contradicting the definition of y_m . Thus $p^a q^b \leq p^i q^j$, and (20) is established.

Accordingly, $j = \lfloor \log_p m - i\rho \rfloor \leq \bar{a}$, so that $y_m/p^{\bar{a}}$ is an element of E . Therefore, $y_m/p^{\bar{a}} \leq m/p^{\bar{a}}$ implies $y_m/p^{\bar{a}} \leq \lfloor m/p^{\bar{a}} \rfloor = \bar{m}$, which in turn implies $\lfloor m/p^{\bar{a}} \rfloor \leq z_{\bar{m}}$. We thus get

$$y_m \leq p^{\bar{a}} z_{\bar{m}} \leq p^{\bar{a}} \bar{m} \leq m.$$

Let $z_{\bar{m}} = p^a q^b$. To conclude the proof by using (20) again, it suffices to show that $b \leq m_\ell$. Since $p^{\bar{a}} q^{m_\ell} \in Z_m$, we have $p^{\bar{a}} q^{m_\ell} \leq m < p^{\bar{a}} q^{m_\ell+1}$, so that $q^{m_\ell} \leq \bar{m} < q^{m_\ell+1}$. Thus $\lfloor \log_q \bar{m} \rfloor = m_\ell$, whence $b \leq m_\ell$ by Lemma 2. \square

Comparing with Proposition 3, characterization (20) of y_m no more depends on z_m . Moreover, it provides a first improvement of Lemma 3.

Corollary 2. *For all $m \in \mathbb{N}$, we have*

$$\frac{G(m)}{y_m} \sim \frac{p}{p-1} \quad \text{as } m \rightarrow \infty. \quad (21)$$

Proof. For $m \in \mathbb{N}$, let $y_m = p^{a_m} q^{b_m}$. According to (17) we have

$$\frac{G(m)}{y_m} - \frac{p}{p-1} = -\frac{k_m}{p^{a_m}}, \quad \text{where } k_m = \frac{q-p}{(p-1)(q-1)} + \frac{1}{q^{b_m}(q-1)}.$$

Observe that $k_m \in \left(\frac{q-p}{(p-1)(q-1)}, \frac{1}{p-1} \right]$ is uniformly bounded. To conclude the proof, we need to prove that $a_m \rightarrow \infty$ as $m \rightarrow \infty$. According to Th. 2, we have $b_m \leq m_\ell$, thus $a_m \geq \ell_{m_\ell}$. Since m_ℓ goes to infinity with m , and since ℓ is non-decreasing and unbounded by Th. 1, a_m goes to infinity with m too. Hence the claim. \square

According to the latter result and Proposition 2, the final task consists in showing that $y_m \sim z_m$. This is done next, so that our main claim is established.

Theorem 3. *For all $m \in \mathbb{N}$, we have*

$$\frac{G(m)}{m} \sim \frac{p}{p-1} \quad \text{as } m \rightarrow \infty.$$

Proof. Assume $y_m \neq z_m$. According to Th. 2, the elements in Z_m that exceed y_m are of the form $p^i q^j$ with $m_\ell < j \leq \lfloor \log_q m \rfloor$. Let us sort these elements together with y_m in an increasing sequence $(n_i)_{i \in [0, N]}$, so that $n_0 = y_m$ and $n_N = z_m$. Notice that the elements of this sequence are consecutive elements of E for the usual order. As soon as m is large enough, we know by Tijdeman's result already mentioned [6] that $n_{i+1} - n_i \leq n_i / (\log n_i)^C$ for an explicitly computable constant $C > 0$. Therefore,

$$z_m - y_m \leq \sum_{i=0}^{N-1} \frac{n_i}{(\log n_i)^C} \leq \sum_{i=0}^{N-1} \frac{p y_m}{(\log \frac{m}{p})^C}.$$

Accordingly, for all $m \in \mathbb{N}$,

$$0 \leq z_m - y_m \leq (\lfloor \log_q m \rfloor - m_\ell) \frac{p y_m}{(\log \frac{m}{p})^C}. \quad (22)$$

At this point, what remains to be proved is that $\lfloor \log_q m \rfloor - m_\ell$ grows asymptotically slower than $(\log \frac{m}{p})^C$ so that $z_m \sim y_m$, and to conclude using (21) and Lemma 2. Recall that m_ℓ is defined as the largest value b such that $p^{\ell_b} q^b \leq m$. Therefore, we have

$$p^{\ell_{m_\ell}} q^{m_\ell} \leq m < p^{\ell_{m_\ell+1}} q^{m_\ell+1},$$

or equivalently, using $\rho = \log q / \log p$,

$$\frac{\ell_{m_\ell}}{\rho} + m_\ell \leq \log_q m < \frac{\ell_{m_\ell+1}}{\rho} + m_\ell + 1, \quad (23)$$

so that

$$\lfloor \log_q m \rfloor - m_\ell < \frac{\ell_{m_\ell+1}}{\rho} + 1. \quad (24)$$

It thus remains to evaluate the terms in sequence ℓ . For that purpose, we first give an explicit formula for ℓ , valid at the jumps of ℓ . We claim that for all $b \in \mathbb{N}^*$,

$$\ell_b > \ell_{b-1} \quad \Rightarrow \quad \ell_b = \left\lfloor \log_p \frac{(q-p)(q^b-1)}{(q-1)(q^b-p^{\lfloor b\rho \rfloor})} \right\rfloor. \quad (25)$$

Indeed, assume that $\ell_b > \ell_{b-1}$. Then, for all $p^i q^j \in Z_{p^{\ell_{b-1}} q^{b-1}}$, we know from (9) that

$$p^{\ell_{b-1}} q^{b-1} - p^i q^j > r(q^{b-1} - q^j).$$

Multiplying both sides of the above inequality by q yields, for all $p^i q^j \in q Z_{p^{\ell_{b-1}} q^{b-1}}$,

$$p^{\ell_{b-1}} q^b - p^i q^j > r(q^b - q^j).$$

Now, $\ell_b > \ell_{b-1}$ implies that there exists an element $p^i q^j \in Z_{p^{\ell_{b-1}} q^b}$ for which the latter inequation does not hold. By Lemma 2 and the definition of Z_{qm} in (5), this element must be $p^{\ell_{b-1} + \lfloor b\rho \rfloor}$, so that

$$p^{\ell_{b-1}} (q^b - p^{\lfloor b\rho \rfloor}) \leq r(q^b - 1).$$

In fact, note that this inequality does not only hold for $p^{\ell_{b-1}}$; by definition of ℓ , it remains valid for $p^{\ell_{b-1}+1}, \dots, p^{\ell_b} - 1$. Accordingly, we get

$$p^{\ell_b-1} (q^b - p^{\lfloor b\rho \rfloor}) \leq r(q^b - 1) < p^{\ell_b} (q^b - p^{\lfloor b\rho \rfloor}),$$

which proves claim (25).

It follows from (25) that, for any b such that $\ell_b > \ell_{b-1}$,

$$\ell_b < \log_p \frac{q^b}{q^b - p^{\lfloor b\rho \rfloor}}. \quad (26)$$

Using another result of Tijdeman (see Th. 1 in [7]), we know that, as soon as $p^{\lfloor b\rho \rfloor} > 3$, there exists another explicit constant $C' > 1$ such that

$$q^b - p^{\lfloor b\rho \rfloor} \geq \frac{p^{\lfloor b\rho \rfloor}}{(\log p^{\lfloor b\rho \rfloor})^{C'}}. \quad (27)$$

Therefore, since $q^b = p^{b\rho}$, (26) and (27) imply that

$$\ell_b < \log_p \frac{q^b (\log p^{\lfloor b\rho \rfloor})^{C'}}{p^{\lfloor b\rho \rfloor}} = \{b\rho\} + \frac{C'}{\log p} \log p^{\lfloor b\rho \rfloor} < 1 + \frac{C'}{\log p} \log \log q^b. \quad (28)$$

Putting all this together, we get the claimed result. Indeed, let b be the smallest index such that $\ell_{m_\ell+1} = \ell_b$. Since $\ell_b > \ell_{b-1}$, we have

$$\ell_{m_\ell+1} = \ell_b < 1 + \frac{C'}{\log p} \log \log q^b \leq 1 + \frac{C'}{\log p} \log \log q^{m_\ell+1} \leq 1 + \frac{C'}{\log p} \log \log qm. \quad (29)$$

Using (24) we get

$$\lfloor \log_q m \rfloor - m_\ell < 1 + \frac{1}{\rho} + \frac{C'}{\log q} \log \log qm = o\left((\log m/p)^{C'}\right), \quad (30)$$

which implies, using (22), that $y_m \sim z_m$ and concludes the proof. \square

Note that the above proof mainly relies on the fact that the sequence ℓ is non-decreasing and that, due to the lower bound in (27) essentially, it grows very slowly. The theorem of Tijdeman that provides this lower bound hinges on a result of Fel'dman about linear forms in logarithms. More recent results of Laurent et alii [8] about such forms in two logarithms allow one to make precise the value of the effective constant C' in (27). Nevertheless, the algorithm presented in the next Section does not make use of (30) in order to compute m_ℓ in logarithmic time.

6. COMPUTING y_m AND $G(m)$ IN $\log \log m$ TIME

Making use of the mapping h , computing $G(m)$ is straightforward as soon as an element of Y_m is known, in particular y_m . According to Theorem 2, $y_m/p^{\bar{a}}$ is the greatest element of $Z_{\bar{m}}$, where \bar{a} and \bar{m} depend on m_ℓ . Once the latter value is known, computing the greatest element in $Z_{\bar{m}}$ can be done in logarithmic time with an algorithm explained in [9].

According to Corollary 1, m_ℓ may be effectively computed if an efficient way of computing the mapping β is found. We shall see that the $\beta(a)$'s are denominators of convergents of ρ , which already improves the computation time. But we shall also see that the latter property implies that the relation $\ell_b = \lfloor \alpha(b) \rfloor$, see (15), also holds for *all* denominators of both even convergents of ρ and their mediants. This allows computing m_ℓ even more quickly by only using a simplified version of the mapping α and binary search.

Note that the convergents of ρ are also of use for the algorithm in [9]. Let us first recall some well known facts about them (see, e.g., [10] or [5]). Let $[a_0, a_1, \dots]$ be the regular continued fraction converging to ρ , and denote by h_i/k_i the i^{th} principal convergent of ρ ($i \geq 0$). The sequences (h_{2i}/k_{2i}) and (h_{2i+1}/k_{2i+1}) are adjacent, converge to ρ , and $(k_i + k_{i+1})^{-1} < |k_i\rho - h_i| < k_{i+1}^{-1}$. Given $i \geq 0$, the intermediate convergents of h_i/k_i , sometimes referred to as mediants, are the rational numbers $h_{i,j}/k_{i,j}$, for $0 < j < a_{i+2}$, given by

$$h_{i,j} = h_i + jh_{i+1}, \quad k_{i,j} = k_i + jk_{i+1}. \quad (31)$$

Let us denote by $(H_n/K_n)_{n \in \mathbb{N}}$ the increasing sequence of all convergents of ρ of even index together with their intermediate convergents. It is known ([11], Th. 2) that (H_n/K_n) is the best lower approximating sequence of ρ , that is, its terms are characterized by the following property. For each $n \in \mathbb{N}$ and integers h, k ,

$$\frac{H_n}{K_n} < \frac{h}{k} < \rho \implies k > K_n. \quad (32)$$

Two immediate consequences are needed here. The first one is that, while the sequence (K_n) increases to infinity, the sequence $(\{K_n\rho\})$ decreases to 0. Indeed, property (32) implies that $H_n = \lfloor K_n\rho \rfloor$, so that (31) implies, for $0 \leq j < a_{i+2}$,

$$\{k_{2i,j+1}\rho\} - \{k_{2i,j}\rho\} = k_{2i+1}\rho - h_{2i+1} \in (-1/k_{2i+2}, 0). \quad (33)$$

The second one rephrases the sufficient condition in (32): If $\{b\rho\} \leq \{j\rho\}$ holds for all integers j such that $0 < j \leq b$, then b is a term of (K_n) . Indeed, let h, k be such that

$$\frac{\lfloor b\rho \rfloor}{b} < \frac{h}{k} < \rho.$$

Since $h < k\rho$, the above inequalities still hold for $h = \lfloor k\rho \rfloor$, which implies $\{k\rho\} < \frac{k}{b}\{b\rho\}$. Supposing $k \leq b$ yields $\{k\rho\} < \{b\rho\}$, a contradiction, so that $\lfloor b\rho \rfloor/b$ satisfies (32).

Now our previous claims may be established.

Theorem 4. *For all $a \in \mathbb{N}$, $\beta(a)$ is a term of the sequence $(K_n)_{n \in \mathbb{N}}$. Moreover, for each $K \in (K_n)_{n \in \mathbb{N}}$, $\ell_K = \lfloor \alpha(K) \rfloor$.*

Proof. Since the sequence $(\phi_{a,i})$ increases from 0 with i and the sequence $(\{K_i\rho\})$ decreases to 0, there is a unique n such that $\{K_n\rho\} < \phi_{a,K_n}$ and $\{K_i\rho\} \geq \phi_{a,K_i}$ for all $i < n$, if any. In particular, $K_n \geq \beta(a)$. We next establish that $K_n = \beta(a)$. This is clear if $n = 0$ since $K_0 = 1$ and $\beta(a) \geq 1$, so assume $n \geq 1$ in the sequel.

Let $b = \beta(a)$ for short, and suppose $b < K_n$. Let $K = K_{n-1}$ for short again, and let $c = \min\{j > 0 : \{j\rho\} < \{K\rho\}\}$. For all $i < c$ we have $\{i\rho\} \geq \{K\rho\} > \{c\rho\}$, so that $c \in (K_i)$, which implies $c = K_n$ since (K_i) decreases. Therefore, $b < K_n$ forces $\{b\rho\} \geq \{K\rho\}$, so that

$$\phi_{a,b} > \{b\rho\} \geq \{K\rho\} \geq \phi_{a,K}. \quad (34)$$

Since $\phi_{a,i}$ increases with i , we get $K < b < K_n$. Property (32) implies that $\lfloor b\rho \rfloor/b < \lfloor K_n\rho \rfloor/K_n$. Since we cannot have $\lfloor K\rho \rfloor/K < \lfloor b\rho \rfloor/b < \lfloor K_n\rho \rfloor/K_n$ ([11], (ii) of Lem. 1), it follows that $\lfloor b\rho \rfloor/b < \lfloor K\rho \rfloor/K$, that is, $\{b\rho\}/b > \{K\rho\}/K$. Thus

$$\{b\rho\} - \{K\rho\} > \frac{b-K}{K}\{K\rho\} \geq \frac{\phi_{a,K}}{K} > \frac{\alpha(1-q^{-K})}{K \log p}.$$

Nevertheless,

$$\phi_{a,b} - \phi_{a,K} < \phi_{a,\infty} - \phi_{a,K} = \log_p \left(1 + \frac{\alpha}{1-\alpha} q^{-K} \right) < \frac{\alpha}{(1-\alpha)q^K \log p}.$$

According to (34) we should thus have

$$\frac{(1-q^{-K})}{K} < \frac{1}{(1-\alpha)q^K},$$

which would imply

$$q-1 < \frac{q^K-1}{K} < \frac{1}{1-\alpha} \leq \frac{p(q-1)}{q(p-1)} < q-1.$$

Therefore, $K_n = \beta(a)$ as claimed, which proves the first assertion of the Theorem.

Next turn to the second one, and let $K \in (K_n)$. On the one hand, $\ell_K \leq \lfloor \alpha(K) \rfloor$ holds. Indeed, there is a unique jump index K^* of ℓ such that $\ell_K = \ell_{K^*}$, and $K^* \leq K$ because ℓ is non-decreasing. According to the first assertion of the Theorem, $K^* \in (K_n)$. Since (K_n) increases and $(\{K_n\rho\})$ decreases, $(\alpha(K_n))$ is increasing, thus $(\lfloor \alpha(K_n) \rfloor)$ is non-decreasing. Therefore, $\ell_K = \ell_{K^*} = \lfloor \alpha(K^*) \rfloor \leq \lfloor \alpha(K) \rfloor$. On the other hand, we also have $\lfloor \alpha(K) \rfloor \leq \ell_K$. Indeed, letting $a = \lfloor \alpha(K) \rfloor$ for short, we have $a \leq \alpha(K)$, that is,

$$p^a \leq \frac{(q-p)(q^K-1)}{(q-1)(q^K-p^{\lfloor K\rho \rfloor})}.$$

Recalling (9), this also reads

$$(p^{a-1}q^K - p^{a-1+\lfloor K\rho \rfloor}) \leq r(q^K-1).$$

Since $\ell_K \geq 0$, we may assume $a \geq 1$. Letting $a' = a + \lfloor K\rho \rfloor$, the above inequality means that

$$h(a-1, K) \leq h(a'-1, 0).$$

Finally notice that $p^{a'-1} < p^{a-1}q^K$. Therefore, $Y_{p^{a-1}q^K} \neq \{p^{a-1}q^K\}$, so that $a-1 < \ell_K$ by (10). Whence $\lfloor \alpha(K) \rfloor = a \leq \ell_K$ as claimed. \square

We may thus use the following algorithm in order to compute m_ℓ given m , p , and q .

1. Compute the denominators k_i of the primary convergents of ρ until finding the largest one with even index, say $k^* = k_{2i}$, that satisfies $p^{\ell_{k^*}} q^{k^*} \leq m$.
2. Compute the largest j such that $K^* = k_{2i,j}$ satisfies $p^{\ell_{K^*}} q^{K^*} \leq m$.
3. Return $m_\ell = \lfloor \log_q m - \ell_{K^*}/\rho \rfloor$.

Let us finally evaluate the number of operations required for these computations. Since $k_i \geq 2^i$, Step 1 requires computing $O(\log \log m)$ values. Each of them obtains in $O(1)$ time using any standard formula for generating the a_i 's and the k_i 's. Checking the stopping conditions in Steps 1 and 2 requires computing $\ell_k = \alpha(k)$, but this may be done in $O(1)$ time without computing q^k . Indeed, let

$$\hat{\alpha}(b) = \log_p \frac{q-p}{q-1} - \log_p(1 - p^{-\{b\rho\}}) = \alpha(b) - \log_p(1 - q^{-b}).$$

Since $\hat{\alpha}(b) - \alpha(b)$ lies in the interval $(\frac{1}{q^b}, \frac{1}{q^{b-1}})$, for each $K \in (K_n)$ we either have $\ell_K = \hat{\alpha}(K)$ or $\ell_K = \hat{\alpha}(K) - 1$. Therefore, any K satisfying $p^{\alpha^+(K)} q^K > m$ also satisfies $p^{\ell_K} q^K > m$. So α is only needed to compute the true value of ℓ two times, in order to check ℓ_{k^*} and ℓ_{K^*} . This is done in $O(\log \log m)$. Finally, there might be a large number of j -values to be coped with in Step 2, but this can also be done in $O(\log \log m)$ time using binary search.

REFERENCES

- [1] V. Dimitrov, G. A. Jullien, and W. C. Miller. Theory and applications of the double-base number system. *IEEE Transactions on Computers*, 48(10):1098–1106, 1999.
- [2] V. Dimitrov, Laurent Imbert, and P. K. Mishra. The double-base number system and its application to elliptic curve cryptography. *Mathematics of Computation*, 77(262):1075–1104, 2008.
- [3] P. Erdős and J. H. Loxton. Some problems in partitio numerorum. *Journal of the Australian Mathematical Society, Series A*, 27(3):319–331, 1979.
- [4] Laurent Imbert and Fabrice Philippe. Strictly chained (p, q) -ary partitions. *Contributions to Discrete Mathematics*, 5(2):119–136, 2010.
- [5] Jean-Paul Allouche and Jeffrey Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, 2003.
- [6] Robert Tijdeman. On the maximal distance between integers composed of small primes. *Compositio Mathematica*, 28(2):159–162, 1974.
- [7] Robert Tijdeman. On integers with many small prime factors. *Compositio Mathematica*, 26(3):319–330, 1973.
- [8] M. Laurent, M. Mignotte, and Y. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *Journal of Number Theory*, 55:285–321, 1995.
- [9] Valérie Berthé and Laurent Imbert. Diophantine approximation, Ostrowski numeration and the double-base number system. *Discrete Mathematics and Theoretical Computer Science*, 11(1):153–172, 2009.
- [10] Serge Lang. *Introduction to Diophantine Approximations*. Springer, 1995.
- [11] Ian Richards. Continued fractions without tears. *Mathematics Magazine*, 54(4):163–171, 1981.

INSTITUT FÜR GENETIK, UNIVERSITÄT ZU KÖLN, GERMANY

E-mail address, F. Disanto: **disafili@yahoo.it**

LIRMM, CNRS, UNIVERSITÉ MONTPELLIER 2, FRANCE

E-mail address, L. Imbert: **Laurent.Imbert@lirmm.fr**

LIRMM, CNRS, UNIVERSITÉ MONTPELLIER 2, UNIVERSITÉ MONTPELLIER 3, FRANCE

E-mail address, F. Philippe: **Fabrice.Philippe@lirmm.fr**